ABSTRAK

Keamanan informasi merupakan aspek krusial dalam menjaga keberlangsungan operasional dan kepercayaan terhadap sistem informasi, terlebih dengan meningkatnya ancaman siber yang semakin kompleks. LEMBAGA XYZ sebagai instansi yang mengelola data sensitif memiliki urgensi untuk memastikan kesiapan keamanan informasinya agar selaras dengan standar internasional. Namun, dalam praktiknya ditemukan sejumlah permasalahan, antara lain belum terdokumentasinya beberapa kebijakan penting serta pelaksanaan kegiatan keamanan yang belum sepenuhnya terstruktur. Penelitian ini bertujuan untuk menganalisis tingkat kesiapan dokumentasi dan pelaksanaan kegiatan keamanan informasi di LEMBAGA XYZ berdasarkan standar ISO/IEC 27001:2022. Metode yang digunakan adalah pendekatan kualitatif dengan teknik analisis kesenjangan (gap analysis) serta penilaian berbasis checklist ISO terhadap kontrol dan klausa yang relevan. Asesmen dilakukan sebanyak tiga kali iterasi untuk memastikan akurasi dan validasi terhadap temuan yang diperoleh. Hasil akhir menunjukkan bahwa LEMBAGA XYZ belum memenuhi 3 dari 10 klausa utama ISO 27001:2022. Kesenjangan ini terlihat dari ketiadaan dokumentasi yang memadai serta kurangnya mekanisme evaluasi dan tindak lanjut yang terstruktur. Sehingga, LEMBAGA XYZ perlu melakukan perbaikan pada aspek dokumentasi kebijakan, pelaksanaan kontrol keamanan, serta siklus evaluasi dan peningkatan berkelanjutan untuk mencapai kepatuhan penuh terhadap ISO/IEC 27001:2022. Rekomendasi strategis diberikan untuk menutup kesenjangan tersebut dan meningkatkan kesiapan lembaga dalam menghadapi sertifikasi keamanan informasi serta manajemen risiko secara menyeluruh.

Kata Kunci: Keamanan Informasi, ISO 27001:2022, LEMBAGA XYZ, Analisis Kesenjangan, Penilaian Kepatuhan